National Cyber Security Centre
a part of GCHQ

Ransomware

Prevention & recovery

Following this advice can reduce the likelihood of you becoming a victim of ransomware. Ransomware makes your data or computers unusable and asks you to make a payment to release it. If your computer is already infected with ransomware, we've included some useful recovery steps below. For more information, please refer to **www.ncsc.gov.uk/ransomware** .



What is ransomware?

Ransomware is malicious software that prevents you from accessing your computer (or data that is stored on your computer).

If your computer is infected with ransomware, the computer itself may become **locked**, or the data on it might be **stolen**, **deleted** or **encrypted**.

Normally you're asked to make a payment (the ransom), in order to 'unlock' your computer (or to access your data).

However, even if you pay the ransom, there is no guaranteethat you will get access to your computer, or your files. This is one of the reasons why it's important to **always have a recent backup** of your most important files and data.

© Crown Copyright 2020

Don't be blackmailed - keep a backup!

If you have a recent backup of your most important files, then you can't be blackmailed.

Make regular backups of your most important files (such as photos and documents), and check that you know how to restore the files from the backup. If you're unsure how to do this, you can search online.

Make sure the device containing your backup (such as an external hard drive or a USB stick) is not permanently connected to your computer.

Turn on auto-backup so that data on your smartphone is automatically copied to the cloud. This means you'll be able to recover your data quickly by signing back into your account from another device.

Protecting your data and devices

The following steps will reduce the likelihood of your devices being infected with ransomware.



Keep your operating system and apps up to date. Apply software updates promptly to help keep your device secure. This includes protection from ransomware and other types of virus. Set updates to happen automatically, so you don't forget.

Make sure your antivirus product is turned on and up to date. Windows and macOS have built in malware protection tools which are suitable for this purpose.

Avoid downloading dodgy apps. Only use official app stores (like Google Play or the Apple App Store), which provide protection from viruses.

What to do if you are infected

If your computer has been infected by ransomware (or any type of malware), you should:



Open your antivirus (AV) software, and run a full scan. Follow any instructions given. If your AV can't clean your device, you'll need to perform a 'clean re-install', which will remove all your personal files, apps and settings. If you're unsure how to do this, you can search online using another device, or ask family and friends.

Restore your backed-up data that you have kept on a separate device (such as USB stick, external hard drive) or cloud storage. Do not copy any data from the infected computer.

If you receive a phone call offering help to clean up your computer, hang up immediately (this is a common scam).

Anyone who thinks they may have been subject to a ransomware attack should contact Report Fraud (www.reportfraud.police.uk). Organisations should call 0300 123 2040. In Scotland, contact the police by dialing 101.

Should I pay the ransom?



Law enforcement do not encourage, endorse, nor condone the payment of ransom demands. If you do pay the ransom:

- **there is no guarantee that you will get access to your data or computer**
- **your computer will still be infected**
- **you will be paying criminal groups**
- **you're more likely to be targeted in the future**

If you have paid any extortion demands you should report this to your local police force.